ABSTRACT

Packet filters and network virtualization are used to restrict network communications. A network mediator corresponding to a computing device uses packet filters to restrict network communications. The network mediator includes a set of one or more filters, each filter having parameters that are compared to corresponding parameters of a data packet to be passed through the network mediator (either from or to the computing device). The network mediator determines whether to allow the data packet through based on whether the data packet parameters match any filter parameters. The set of filters can be modified by a remote device, but cannot be modified by the computing device whose communications are being restricted (thereby preventing the device whose communications are being restricted from being able to modify those restrictions). Additionally, the set of filters may be modified by remote devices at different managerial levels, although remote devices are prohibited from modifying filters to make the filters less restrictive than filters imposed by higher level devices. Network virtualization can be also be used, either in addition to or in combination with the packet filters, to restrict network communications by the network mediator maintaining a mapping of virtual addresses to network addresses, and allowing the computing device to access only the virtual addresses. When a data packet is sent from the computing device, the data packet will include the virtual address which is changed to the network address by the network mediator prior to forwarding the packet on the network. Similarly, when a data packet is received at the network mediator targeting the computing device, the network mediator changes the network address in the data packet to the corresponding virtual address. By virtualizing the addresses, the computing device is restricted in its

knowledge and ability to access other devices over the network because it has no knowledge of what the other devices' addresses are.